



**SIMPLIFIED ADMINISTRATION,
CENTRALIZED MANAGEMENT,
ORGANIZATIONAL INSIGHT
AND ASSURED COMPLIANCE**

IronPort Email Security Appliance Management

OVERVIEW

IronPort C-Series™ email security appliances offer industry-leading protection against email-borne malware threats such as virus, spam and botnets. The *IronPort M-Series™* security management appliances provide advanced technology to centrally manage the reporting, tracking and *IronPort Spam Quarantine™ (ISQ)* for multiple *IronPort C-Series* appliances.

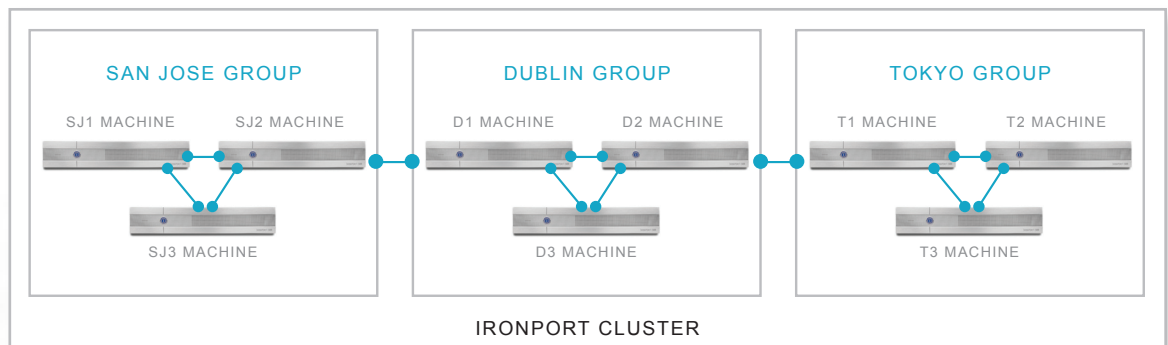
Built on IronPort's industry-leading *AsyncOS™* platform, *IronPort M-Series* appliances offer robustness and scalability to satisfy the needs of the largest enterprises in the world. With zero administration, self-service features, an intuitive interface and actionable reports, IronPort® provides significant value to organizations.

FEATURES

Centralized Management provides peer-to-peer configuration for multiple *IronPort C-Series* appliances. This versatile feature reduces administrative overhead and ensures a uniform configuration across the network.

IronPort C-Series appliances can be deployed as a cluster – where each cluster represents a logical group of appliances that share

common configuration settings. Centralized management facilitates the administration of different elements of the system on a cluster-wide, group-wide, or per-machine basis. This flexibility and granularity enables the segmentation of appliances based on network, geography, business unit or any other logical relationship.



Centralized management of IronPort C-Series appliances

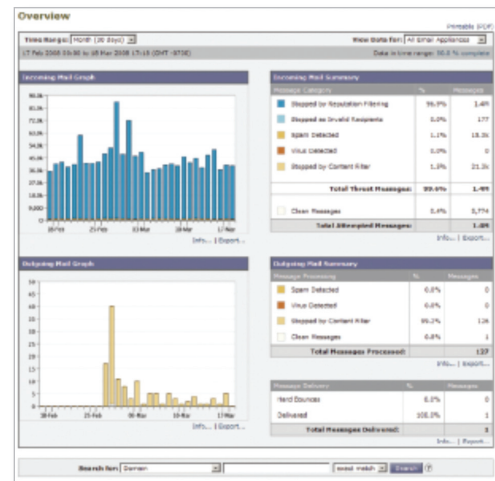


FEATURES (CONTINUED)

Centralized Reporting on the *IronPort M-Series* appliance consolidates reporting data from multiple *IronPort C-Series* appliances. Actionable reports provide a unified view of all email traffic, malware threats, user behavior and critical content security policies across the organization at various levels of granularity.

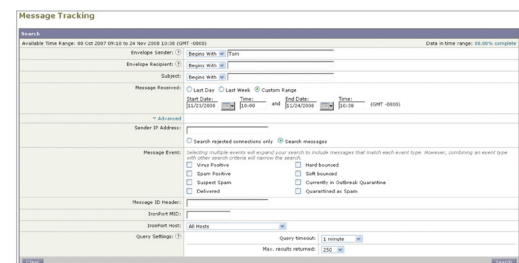
Centralized reports give a complete picture of the state of an organization from the perspective of email traffic and email-borne threats. Security reports provide insight into the malware threats faced by an organization both inside and outside its perimeter. Critical content security policy and internal user behavior reports enable visibility into an organization’s compliance requirements. The domain-based executive summary report provides a summarized view of incoming and outgoing message traffic, spam and virus volumes on a per-domain basis. This multi-dimensional and holistic view across multiple *IronPort C-Series* appliances enables faster analysis and decisions.

IronPort’s powerful reporting engine allows organizations to capture the current view of any report in an Adobe PDF file, schedule reports to be automatically emailed, or (for easy integration with existing monitoring solutions) download the reporting data in CSV format. With reports centralized to show data over a longer timeframe than on an *IronPort C-Series* appliance, the *IronPort M-Series* provides demonstrable business value.



Centralized Overview reports on the IronPort M-Series

Centralized Message Tracking enables administrators to easily answer questions such as, “What happened to that email I sent two hours ago?” from a single console. Administrators can now find out where, and when, an email communication took place. A powerful search feature tracks messages across multiple *IronPort C-Series* appliances by time, sender, recipient, message subject and other advanced parameters such as message handling events, delivery details (including spam/virus scan verdicts), policy violations, TLS statistics, DKIM, *IronPort PXE™* and content filters. Search results can be exported for further analysis and message details are available as a PDF. An intuitive search interface, combined with time-saving features such as a single click refinement of search results, vastly reduces administrative burden.

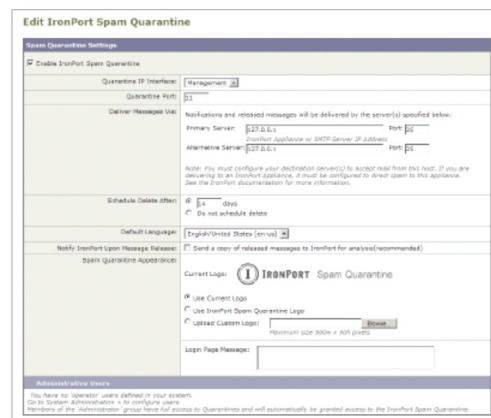


Centralized Message Tracking



The **IronPort Spam Quarantine** boasts a centralized, self-service Web or email-based interface with simple integration into existing directory and mail systems. *IronPort C-Series* appliances can deliver spam to an *IronPort M-Series*, where it is then aggregated into a centralized spam quarantine that is accessible to end-users.

End-users can be authenticated against corporate LDAP directories or IMAP and POP messaging servers. Additionally, end-users can manage their own spam quarantines by creating personal safelists and blocklists. End-users can also consolidate and look at multiple email addresses or proxy accounts with a single login. The *IronPort Spam Quarantine* requires virtually no maintenance by the administrator or the end-user.



Centralized spam quarantine on the IronPort M-Series

Redundant Data Aggregation allows organizations to deploy their network in a redundant topology, whereby the *IronPort C-Series* appliances can send email reporting and tracking data to two separate *IronPort M-Series* appliances. This topology provides redundancy and failsafe backup for the *IronPort M-Series* appliances.

BENEFITS

Simplified Email Security Administration IronPort’s intuitive interface makes deployment of the *IronPort C-Series* and *IronPort M-Series* appliances easy, smooth and hassle-free. The centralized management features for the *IronPort C-Series* simplifies overall management, reporting and auditing of the email security network and reduces administrative overhead.

Security Budget Optimization Reporting data, message tracking information and spam quarantine details can all be managed by the *IronPort M-Series* – letting you dedicate your other appliances to keeping security threats at bay.

Increased Email Security Visibility The *IronPort M-Series* appliances can aggregate information from all of the email security appliances in your network. Centralized reports (such as CEO-friendly domain-based overview reports), centralized message tracking and centralized spam quarantines provide valuable insights into the email traffic of the entire corporate network.

Assured Compliance The *IronPort M-Series* provides detailed information on policy violations, filter matches, and user activity – even for events that may have occurred months or years ago. This long-term visibility allows CIOs and administrators to react quickly to requests for trend analyses and audits, which are critical when responding to governance and compliance requirements.



FEATURE COMPARISON

Feature	IronPort C-Series	IronPort M-Series
Interactive Reports	Yes	Yes
Message Tracking	Yes	Yes
IronPort Spam Quarantine	Yes	Yes
Peer-Peer Cluster Management	Yes	-
Centralized Reporting	-	Yes
Domain Based Summary Reports	-	Yes
Centralized Message Tracking	-	Yes
Centralized Spam Quarantine	-	Yes
Data Redundant Deployment	-	Yes
Visibility into all Appliances in the network	-	Yes
Reporting and Tracking Visibility*	1 month	1 year

*Assumes typical email traffic for an enterprise-class customer

PRODUCT LINE

IronPort Systems provides industry-leading email and Web security products for organizations ranging from small businesses to the Global 2000.

IronPort M1060™	Consolidated management appliance designed to meet the needs of the most demanding networks in the world.
IronPort M660™	Suggested for organizations with multiple gateway security appliances and thousands of users.
IronPort M160™	Designed for organizations with multiple gateway security appliances and less than 2000 users.

TECHNICAL SPECIFICATIONS

	IronPort M1060	IronPort M660	IronPort M160
Chassis			
Form Factor	19" Rack-Mountable, 2U rack height	19" Rack-Mountable, 2U rack height	19" Rack-Mountable, 1U rack height
Dimensions	3.5" (h) x 17.5" (w) x 29.5" (d)	3.5" (h) x 17.5" (w) x 29.5" (d)	1.75" (h) x 17.5" (w) x 21.5" (d)
Power Supplies	750 watts, 100/240 volts	750 watts, 100/240 volts	345 watts, 100/240 volts
Processor, Memory, and Disks			
CPUs	2x4 (Quad Cores) Intel XEON	2x4 (Quad Cores) Intel XEON	1x2 Dual Core Intel Xeon
Disk Space	3 TB	1.8 TB	500 GB
RAID	RAID 10, battery-backed 256MB cache	RAID 10, battery-backed 256MB cache	RAID 1, battery-backed 256MB cache
Interfaces			
Ethernet	3xGigabit NICs, RJ-45	3xGigabit NICs, RJ-45	2xGigabit NICs, RJ-45
Fiber	Yes	No	No
Web Interface	GUI-based (HTTP or HTTPS)	GUI-based (HTTP or HTTPS)	GUI-based (HTTP or HTTPS)

Compatibility: Interfaces with all IronPort gateway security appliances.



SUMMARY

IronPort M-Series security management appliances support the best-of-breed *IronPort C-Series* email security appliances. The *IronPort M-Series* offers a high-performance, robust and scalable platform that provides centralized reporting, message tracking and spam quarantine services. Using the management features from IronPort, CIOs and IT administrators can simplify their email security administration, gain corporate-wide insight into their email network, and satisfy governance and compliance requirements.

CONTACT US

HOW TO GET STARTED WITH IRONPORT

Through a global sales force and reseller network, IronPort offers a free “Try Before You Buy” program. IronPort sales representatives, channel partners and sales engineers are ready to help evaluate how IronPort products can make your corporate network infrastructure secure, reliable and easier to manage. If you believe that your organization could benefit from IronPort’s industry-leading products, please call 650-989-6530 or visit us on the Web at www.ironport.com/try.



IronPort Systems

950 Elm Avenue, San Bruno, California 94066

TEL 650.989.6500 FAX 650.989.6543

EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems, now part of Cisco, is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world’s largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use—providing breakthrough performance and playing a mission-critical role in a company’s network infrastructure.

Copyright © 2000-2009 Cisco Systems, Inc. All rights reserved. IronPort, the IronPort logo and SenderBase are registered trademarks of Cisco Systems, Inc. All other trademarks are the property of Cisco Systems, Inc. or their respective owners. While every effort is made to ensure the information given is accurate, Cisco does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice. P/N 435-0244-1 01/09

IronPort is now
part of Cisco.

